Università degli Studi Roma Tre
Corso di Studi in Matematica
CR410 – Crittografia1
Esercizi
Foglio 3

1. Applicare il test di Miller-Rabin (per max due iterazioni) agli interi $n_1 = 15841$ e $n_2 = 1103$.

   Sol: n_1 supera il test con base $b = 2$: infatti $n_1 - 1 = 2^5 495$, e $2^{495} \equiv 1 \pmod{n_1}$. Non supera il test con base $b = 3$: infatti $3^{495} \not\equiv 1 \pmod{n_1}$, $3^{2\cdot 495} \equiv 218 \pmod{n_1}$ e $3^{4\cdot 495} \equiv 1 \pmod{n_1}$. Quindi n_1 non è primo, e 218 è radice non banale dell'unità modulo n_1. Calcolando $(n_1, 219) = 73$ abbiamo informazioni sulla fattorizzazione di $n_1 = 73 \cdot 217 = 73 \cdot 7 \cdot 43$. Invece n_2 è primo e supera quindi il test sia in base 2 che in base 3: infatti $n_2 - 1 = 2 \cdot 551$, $2^{551} \equiv 1 \pmod{n_2}$ e $3^{551} \equiv 1 \pmod{n_2}$.

2. Sapendo che una versione di RSA ha $N = 10573$, esponente di cifratura $e = 11$ e di decifratura $d = 8483$, fattorizzare N.

   Sol: Si ha $ed - 1 = 93312 = 2^7 729$. Scegliamo come base $b = 2$: abbiamo che $2^{729} \not\equiv \pm 1 \pmod{10573}, 2^{2\cdot 729} \not\equiv \pm 1 \pmod{10573}, \dots 2^{16\cdot 729} \equiv 1 \pmod{10573}$. Ora $2^{8\cdot 729} \equiv 1745 \pmod{10573}$ e troviamo la fattorizzazione calcolando $(1744, 10573) = 107$ e $10573/107 = 97$.

3. Provare che, se n è uno pseudoprimo di Eulero in base b e se $\left(\frac{b}{n}\right) = -1$, allora n è uno pseudoprimo forte in base b.

   Sol: Dalle ipotesi si ha $b^{n-1/2} \equiv \left(\frac{b}{n}\right) = -1$, quindi nel calcolo della lista
   $$b^t, b^{2t} \dots b^{n-1/2}, b^{n-1} \pmod{n}$$
   le ultime due posizioni sono $-1, 1$ e n è uno pseudoprimo forte in base b.

4. Esprimere $21/13$ e $141/79$ come frazioni continue. Calcolare i convergenti di $21/13$. **Sol:** Si ha $21/13 = [1; 1, 1, 1, 1, 2]$ o $[1; 1, 1, 1, 1, 1, 1]$, con convergenti $1, 2, 3/2, 5/3, 8/5, 21/13$; $141/79 = [1; 1, 3, 1, 1, 1, 5]$ o $[1; 1, 3, 1, 1, 1, 4, 1]$.

5. Usando l'attacco di Wiener (delle frazioni continue) trovare la chiave privata del crittosistema RSA che ha $N = 1868077, e = 1356611$.

   Sol: La parte iniziale dello sviluppo di e/N in frazione continua è $[0; 1, 2, 1, 1, 1, 7, 8, \dots]$ e i primi convergenti sono $0, 1, 2/3, 3/4, 5/7, 8/11, 61/84 \dots$

Dal momento che d deve essere dispari, possiamo scartare i convergenti con denominatore pari. Scartiamo $2/3$ perché $d = 3, k = 2$ dà un valore di $(ed-1)/k$ maggiore di N. Provando $d = 7, k = 5$ ottieniamo un valore di $(ed-1)/k$ non intero. Scelti $d = 11, k = 8$ otteniamo $(ed-1)/k = 1865340$. Da $N = 1868077, \varphi(N) = 1865340$ otteniamo l'equazione $x^2 - 2738x + 1868077$ che ha soluzioni $1291, 1447$, e possiamo verificare che $N = 1291 \cdot 1447$.

6. Lo stesso messaggio m è stato cifrato per i tre utenti A_1, A_2, A_3 che hanno chiavi pubbliche RSA rispettivamente $(161, 3)$, $(209, 3)$, $(221, 3)$. I tre testi cifrati ottenuti sono $y_1 = 6, y_2 = 113, y_3 = 177$. Decifrare il messaggio, senza fattorizzare i moduli.

   Sol: Dobbiamo risolvere il sistema di congruenze

$$\begin{cases} x \equiv 6 \pmod{161} \\ x \equiv 113 \pmod{209} \\ x \equiv 177 \pmod{221} \end{cases}.$$

   Possiamo per esempio risolvere il sistema formato dalle prime due congruenze ottenendo la soluzione $x \equiv 29791 \pmod{33649}$, e osservare che 29791 è anche soluzione della terza congruenza, quindi è l'unica soluzione positiva minore di $161 \cdot 209 \cdot 221 = 7436429$. Quindi $m^3 = 29791$, da cui $m = 31$.